AO 91 (Rev. 11/11) Criminal Complaint

Sealed
Public and unofficial staff access to this instrument are prohibited by court order

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.
Gregory Pierre Hayden

Case No. **4:20mj1050**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 11/1/2019 through 4/30/2020 in the county of Fort Bend in the Southern District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
Title 18 U.S.C. Section 1028(a)(7)	Fraud and related activity in connection with identification documents, authentication features, and information
Title 18 U.S.C. Section 1030(a)(5)(A)	Fraud and related activity in connection with computers
18 U.S.C. Section 371	Conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(5)(A)
18 U.S.C. Section 371	Conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(4)

This criminal complaint is based on these facts:

See attached affidavit

☑ Continued on the attached sheet.

Complainant's signature

David Ko-Special Agent
Printed name and title

Sworn to before me telephonically.

Date: June 11, 2020

Judge's signature

City and state: Houston, Texas

Dena Hanovice Palmero, US Magistrate Judge
Printed name and title

Summary

Gregory Pierre Hayden ("Hayden"), along with several co-conspirators were identified taking over victims' cell phones in order to gain unauthorized access to their bank accounts. As such, the FBI now seeks an arrest warrant.

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation and have been since June 2010. I am currently assigned to a criminal cyber squad, where I investigate computer intrusions and other technology-based crimes. As part of my responsibilities, I investigate cybercrimes involving the unauthorized intrusions into a computer, cell phone, or network, and certain technology related frauds. I have received training in computer security and investigations involving computers, cell phones, and the Internet. For example, in addition to 20 weeks at the FBI Academy as a Special Agent, I have several certifications in computer forensics, incident response, cell phone hacking techniques, and cell phone forensics.

2. The facts set forth in this affidavit are based upon Affiant's own personal observations, training, and experience, as well as information obtained during this investigation from other sources including: (a) other agents from the FBI, and other law enforcement personnel involved in this investigation, (b) statements made or reported by various witnesses with personal knowledge of relevant facts; and (c) my review of records obtained during the course of this investigation, as

well as summaries and analyses of such documents and records that have been prepared by others.

3. I make this affidavit in support of an application for a warrant to arrest the defendant for violations of 18 U.S.C. §§ 1028(a)(7) (fraud and related activity in connection with identification documents, authentication features, and information), 1030(a)(5)(A) (fraud and related activity in connection with computers), 371 (conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(5)(A)) and 371 (conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(4)) (collectively, the "Subject Offenses"). Because this affidavit is submitted for the limited purpose of obtaining this arrest warrant, I have not set forth each and every fact I have learned in connection with this investigation. Where conversations and events are referred to herein, they are related in substance and in part, and where figures and calculations are set forth herein, they are approximate.

II. SUMMARY OF PROBABLE CAUSE

4. This application for an arrest warrant is made in connection with an investigation of "SIM-jacking." SIM-jacking is where unknown subjects gain unauthorized access to a victim's phone by fraudulently copying a phone's Subscriber Identification Module card ("SIM card") assigned by the victim's cell phone provider. A SIM card is piece of hardware that

allows a device, like a cellular phone, to communicate with a service provider. The SIM card is what connects the service to an account; essentially, with a SIM card one can make calls, receive texts, and use the Internet from that particular account. Once a subject engaged in SIM-jacking has access to the phone calls and text messages for the phone, s/he is able to exploit the victim's use of two-factor authentication to gain access to the victim's online accounts.

5. The investigation has identified 79 victims who have had their cell phone accounts compromised and, subsequently, attempts were made to access their financial accounts. Based on video surveillance, interviews, application logs, and other investigative techniques, the FBI has identified Hayden, as the person who had conducted the SIM swaps as a Mobilelink LLC ("Mobilelink") employee.

III. STATEMENT OF PROBABLE CAUSE

A. Background Regarding SIM-jacking

6. Hayden and/or other subjects fraudulently copied 79 victims' SIM cards and then exploited a weakness in certain types of two-factor authentication. Two-factor authentication is used by many online providers to increase the security around an online account. One common example is for Gmail, where the online provider (Google) allows a user to turn on two-factor authentication and have a code texted to the user's phone. The user then enters this code when using the Google account to help authenticate that he or she is, in fact, the user, when logging

into the Gmail account from a phone. Additionally, financial institutions will often send a code to the registered cell phone if a password reset request has been made. Hayden and others used this weakness to gain unauthorized access to victims' personal and financial accounts.

7. SIM-jacking occurs when a subject obtains access to the user's cell phone account (the account access is often enabled by the phone's SIM card). This can occur when an employee of the cell phone provider conducts a SIM swap without the victim's knowledge (although there are other ways for a subject to illicitly gain access to the victim's cell phone account).

8. In this instance, Hayden conducted 79 SIM swaps on the victims' accounts. AT&T/Mobilelink confirmed for all 79 SIM swaps, the actual customers notified AT&T/Mobilelink that they had not authorized a SIM swap. Many cell phone providers provide additional security by adding a PIN so that the customer's account cannot be accessed without the PIN. However, employees can bypass the PIN by entering the last four digits of the customer's social security number.

9. Based off past investigations, SIM-jacking subjects often conduct research on the victims prior to the actual SIM swap. Generally, the subjects gain access to the victim's name, date of birth, social security number, address, and other personally identifiable information ("PII"). The PII is then used to validate account information, create other accounts, or socially engineer administrators to gain access. Additionally,

SIM-jacking subjects also may have additional financial information to more efficiently conduct the fraud. With the hack of Equifax data (147 million customers) around September 2017 and Experian around October 2013, many victims' financial data was also compromised and sold online which provided their financial accounts and other information. Investigations show that subjects had documents indicating the financial accounts and amounts of money in each of the victims' accounts.

10. The result of SIM-jacking is that the subject can gain access to virtually all communications sent to the victim's phone – including any two-factor authentication codes that could be used to access the victim's e-mail and financial accounts. Once a subject has successfully SIM-jacked a phone, it is relatively easy for the subject to use the phone to access other online accounts of the victim without authorization.

B. Mobilelink, LLC.

11. Mobilelink, LLC is an authorized Cricket Wireless and AT&T retailer.

12. On May 20, 2020, Mobilelink contacted the FBI regarding SIM swapping activities being conducted by one of their employees, Hayden. Hayden was hired by Mobilelink in January 2019 as a Retail Sales Consultant and worked at the Missouri City, Texas location, which is in the Southern District of Texas.

13. According to AT&T, between November 2019 and April 2020, Hayden conducted 79 suspicious SIM swaps. Based on a preliminary investigation conducted by AT&T, all 79 customers

had called AT&T to report an unauthorized SIM swap on their account. Based on data provided by AT&T/Mobilelink, between November 2019 and May 2020, Hayden's account conducted 212 SIM swaps, of which 81 were determined to be suspicious[1].

14. AT&T and their retailers use a system called OPUS to manage user accounts. AT&T owns the OPUS database and system. Often the sales consultants interact with the OPUS database using a tablet. Each sales consultant has a unique user ID and password which is used to access the database. Customer records are locked with a PIN code to prevent unauthorized access. However, the PIN can be bypassed by a sales consultant by entering in the last four digits of the customer's social security number. Social security numbers are not available to Mobilelink employees through the OPUS database. For all 79 customers, which Hayden's account switched, the PIN had been bypassed using the customer's social security number.

C. Legitimate SIM swap process

15. Based off information provided by AT&T, legitimate SIM card changes (a.k.a SIM swaps) are common occurrences primarily for customers upgrading wireless devices; customers suffering from lost, stolen, damaged wireless devices; customers with technical issues; and/or customers' specific requests.

16. After a legitimate request for a SIM swap, the customer's wireless number is used to access the account. Next the customer provides a valid government-issued photo ID. If

[1] 81 SIM swaps were conducted, two on duplicate accounts resulting in 79 unique victims

the ID has a bar code then it is scanned but can be bypassed and the system will record "DL will not scan" or a similar notation. Then the customer's name is entered followed by the ID and ID card expiration date. Next the passcode for the account is entered. If the passcode is not known or is incorrect, the "forgot/does not know passcode" box is checked in the system and three options are provided. Option 1: a six-digit PIN is sent via text to the active wireless number on the account. Option 2: a PIN is sent to an e-mail address on the account. Option 3: the last for digits of the account holder's Social Security Number are entered for validation and an explanation entered into the system for why the PIN could not be received.

17. After the account has been validated, a SIM card change is initiated by clicking the device that needs the SIM swap and a new SIM card is either scanned or manually entered into the text box below the active SIM card number. After the transaction is submitted, the SIM card change is completed.

18. Prior to starting as an employee at Mobilelink, Hayden was required to take training on the OPUS system and its authorized use. A screenshot of the training provided by Mobilelink stated the following: "Retail is only allowed to authenticate a customer in face-to-face transactions. All customers must present valid, government-issued photo ID with the name on the ID matching the name on the account and image matching the person present." Mobilelink also informed your affiant that any unauthorized SIM swap was not an authorized use of the OPUS database and in violation of the training provided.

D. Six SIM swaps conducted by Hayden on April 14, 2020

19. On April 14, 2020 six fraudulent SIM swaps were conducted by Hayden. Based on logs provided by AT&T/Mobilelink, Hayden's OPUS user account, GH1529, conducted six SIM swaps between 2:00 p.m. and 3:19 p.m. CST. Every SIM swap used Hayden's user account from IP address 50.208.69.2 which is registered to the Mobilelink store where Hayden worked. Based on conversations with AT&T and Mobilelink, once Hayden initiated a transaction on the OPUS database, the information would be transferred from the OPUS tablet to the store router where it would be sent to a server for authentication. AT&T has confirmed that data is stored in redundant locations in varied locations to protect the data against destruction and loss. These locations are purposely placed in distant locations so that a natural disaster would not destroy all of the data. Analysis of the victims' locations also indicated that they resided in numerous states to include Texas, North Carolina, Florida, New York, Michigan, Pennsylvania, Nevada, California, Connecticut, Oklahoma, Georgia, Alabama, New Jersey, Indiana, Montana, West Virginia, and elsewhere. Based on my knowledge and experience, the information from the victims is generally collected at their location and also stored in a number of areas around the world for redundancy purposes which would likely include other locations outside the Southern District of Texas.

20. In order to conduct the SIM swap, Hayden must have had either the customer's PIN or last four of their social security number to authorize the swap. OPUS logs further indicate that the 79 SIM swaps bypassed the user PIN by using the last four digits of the victims' social security number. Based on surveillance video, Hayden appears to have used his cell phone to get the social security information and transferring SIM number. Based on my training and experience, criminals often need to communicate important information to each other such as the social security number for a victim. The most common method of communication is via cell phone, either through text message or another messaging application.

21. On April 14, 2020 at 2:00 p.m. CST, AT&T customer S.C. had been using her cell phone in the O'Fallon, Missouri region when the SIM swap occurred. The cell phone number then became active in the South Florida region where calls were made to Bank of America and Fidelity Investments. Around the time of the swap, S.C. had been using an iPhone XR; once the swap occurred, the account was being used by an iPhone 5C in South Florida. S.C. also received numerous amounts of spam calls moments before the SIM swap occurred which prevented her from calling AT&T. The password on S.C.'s Fidelity bank account was changed and a voice verification code had been set to prevent a password change. Fidelity told S.C. that the person who enabled the voice code had provided the correct name, date of birth, address, and social security number. S.C. successfully prevented any unauthorized activity by freezing the

account. S.C. confirmed that she never used an iPhone 5C nor did she authorize its use. Records from Fidelity Investments indicate that multiple 2FA notifications were sent to S.C.'s registered phone number and the PIN was reset. On April 15, 2020, a person claiming to be S.C. called requesting a $5,400 wire be sent to Ebony Glass, 23027 South West 109th Ave., Miami, FL 33170. Fidelity Investments did not believe the voice was consistent with the account owner and deleted the request before it was completed. Based on surveillance from inside the store located in Missouri City, Texas, when the swap occurred, Hayden was sitting in the store interacting with his cell phone and then using an OPUS tablet. No customers were seen in the store and call records from Mobilelink indicate there was only one call from an unrelated number several minutes before the SIM swap was completed. S.C. confirmed that she did not authorize a SIM swap.

22. On April 14, 2020 at 2:27 p.m. CST, AT&T customer V.O. had been using his cell phone in the Kentucky region when the SIM swap occurred. The cell phone number then became active in the South Florida region. V.O. received a text message that his AT&T service was switching to a new phone and then his phone ceased working. Records from Fidelity Investments indicate that on April 14, 2020 multiple 2FA notifications were sent to V.O.'s registered cell phone number. An individual called Fidelity Investments claiming to be V.O. regarding a wire transfer of $7,432. Fidelity Investments advised that there were insufficient funds and the caller hung up. V.O. confirmed that

he did not call regarding the wire transfer. Around the time of the swap, surveillance video from the store in Missouri City, Texas showed Hayden looking at information on his phone and then interacting with the OPUS tablet. Mobilelink phone records show the only call to the store around the time of the SIM swap was approximately 29 minutes prior. V.O. confirmed that he did not authorize the SIM swap.

23. On April 14, 2020 at 2:38 p.m. CST, AT&T customer L.L. had been using his cell phone in the Corona, California region when the SIM swap occurred. The cell phone number then became active in the South Florida region. L.L. did not authorize the SIM swap and was unaware of anyone who would be using his cell phone number in Florida. After the SIM swap, unknown subjects successfully gained access to L.L.'s Fidelity bank account and attempted to withdraw the total amount in the account, approximately $90,000. Around the time of the SIM swap, surveillance video showed Hayden sitting in the store located in Missouri City, Texas, interacting with his cell phone and the OPUS tablet.

24. On April 14, 2020 at approximately 3:19 p.m. CST, AT&T customer E.M. was using his iPhone 11 in the Big Spring, Texas area when the SIM swap occurred. Once the SIM was completed, the cell phone number then became active in the South Florida area on an iPhone 6S where calls were made to Chase Bank, Square, Citibank, and Chase Bank. E.M. realized his cell phone stopped working on April 14, 2020 but thought it was because he had dropped his phone and believed the SIM card may have become

dislodged. When E.M. came within range of a wireless signal he received an e-mail that his Capital One credit card had been maxed out to $11,000. He also realized that his passwords had changed on his e-mail account and financial accounts. E.M. noted a Zelle transaction from his Chase Bank account to Wells Fargo totaling $4,950. His Venmo account had a wire of $2,500, and his CashApp account had a total of $5,600 of unauthorized transactions. There was also a declined charge for $80 to Verizon and $210 to Best Buy. E.M. neither authorized a SIM swap nor was he aware of an iPhone 6S on his account. Just before the time of the SIM swap, surveillance video inside the Mobilelink store showed Hayden take the OPUS tablet and walk outside to meet an unknown individual. Hayden remained outside out of clear view of the camera for the duration of the SIM swap transaction on E.M.'s account.

25. On April 16, 2020 at approximately 1:11 p.m. CST, AT&T customer C.C. had been using her cell phone in the Chicago, Illinois area on an iPhone 8 prior to the SIM swap. After the SIM swap the account became active in the South Florida region on an Emblem Solutions U202AA phone. C.C. received a text message indicating that her SIM card had been swapped and then the phone lost service. C.C. attempted for several hours to rectify the situation, restoring service on April 18, 2020. C.C.'s Chase bank account password changed and she subsequently froze the account. C.C. neither authorized a SIM swap nor was she aware of anyone in the South Florida region would have had access to her account.

E. Other SIM swaps conducted by GH1529

26. On January 15, 2020, AT&T customer D.K. had been using her cell phone in the Pennsylvania area prior to the SIM swap on an iPhone 10. After the SIM swap occurred, her account became active in the Atlanta, Georgia area. Subsequent to the SIM swap, calls were made to Citibank, Barclays Bank, Home Depot Consumer Credit Card, Lowe's, Capital One, Chase Bank, and AT&T. D.K. noticed her phone was not working and called Barclay Bank who informed her that approximately $14,749 in transactions were attempted at numerous locations to include Walmarts in the Atlanta, Georgia area. D.K. also saw that a Syngony Bank account was opened in her name and a transaction to pay for plastic surgery was attempted. She also received notification that a Home Depot credit card, Wayfare, and Comenity Capital Bank account had been attempted to be opened in her name.

27. On March 23, 2020, AT&T customer J.M. had been using his Samsung Galaxy S7 Active in the Oklahoma City, Oklahoma area prior to the SIM swap. At approximately 7:21 p.m. a SIM swap was conducted, after which the account became active in the South Florida area on an iPhone 6S. A total of $43,301.37 in fraudulent transactions were attempted in J.M.'s Fidelity Investments account and several accounts opened in his name at Wells Fargo, JP Morgan Chase, TD Bank, and GoBank. American Express and Citibank also called J.M. advising of a platinum account owned in his name. Based on information provided by Fidelity Investments, on March 24, 2020 a 2FA code was sent to J.M.'s cell phone and the password was subsequently reset. Then

a wire was initiated for $8,650 to a Wells Fargo Bank account in J.M.'s name. A second wire was initiated for $8,150 to a Citibank account in J.M.'s name. A third wire was initiated to transfer $7,966.37 to a TD Bank account in J.M.'s name. A fourth wire was initiated for $5,675 to a Go Bank account in J.M.'s name. A fifth wire was initiated for $5,190 to a JP Morgan Chase Bank account in J.M.'s name. A sixth wire was initiated for $7,670 to an Evolve Bank and Trust account in J.M.'s name. J.M. was also a cosigner on his daughter's Bank of America account which saw an unauthorized $300 wire. J.M. confirmed that he did not authorize a SIM swap and was not aware of anyone in the South Florida area who he would have authorized to use his phone number. Call logs for the Mobilelink store show no incoming calls received around the time of the swap.

28. On April 2, 2020, AT&T customer K.B. had been using her iPhone X in the Austin, Texas region when her SIM card was swapped and the account became active in the South Florida region on a Samsung SM-G920V. Around the time of the SIM swap, K.B. received a large number of spam e-mails. K.B. used another phone to call AT&T believing that she had forgotten to pay her cell phone bill. After paying the bill, service to her account had not been restored. K.B. attempted to call Fidelity Investments the same day because she had approximately $5 million in the account. Fidelity advised her that there were $49,371.67 in wire attempts on her account which were prevented. Records from Fidelity Investments indicate that on April 2, 2020, a 2FA was sent to K.B.'s registered cell phone. Wire

instructions were added to send $14,468 to a Citibank account in K.B.'s name. A second wire was initiated for $18,300 to a Bank of America account in K.B.'s name. A third was wire was initiated for $16,243.67 to a JP Morgan Chase Bank in K.B.'s name. Between April 2 and April 8, 2020, Fidelity Bank received multiple calls regarding the status of the wire transfers. On her Bank of America account there were numerous Zelle transfers totaling $3,500; which was later reimbursed by Bank of America. K.B. did not authorize a SIM swap on her account nor was she aware of anyone using a Samsung phone in the South Florida area. Call logs for the Mobilelink store show no incoming calls received around the time of the swap.

29. On April 13, 2020, AT&T customer P.B. had been using her phone in the Frisco, Texas area when his SIM card was swapped and his account became active in the South Florida area. Just before the swap, P.B. saw a text message from Fidelity Investments advising of wire attempts made on her account for $9,852 and $4,000. The $9,800 wire went through but the $4,000 attempt was delayed for verification. Records from Fidelity confirmed that on April 13, 2020 2FA was initiated to P.B.'s registered cell phone number. Shortly thereafter a $9,852 wire transfer was processed to a BBVA account in P.B.'s name. A $4,200 wire transfer was initiated to Go Bank in the name of Junior Augustin, 1350 NW 132nd Street, Apartment 200, Miami, FL 33167. Fidelity Investments was able to delete the wire to Go Bank before it was funded. J.M. did not authorize a SIM swap

and did not know anyone in the South Florida region who would have had access to her phone number.

F. Hayden's Cell Phone

30. Based off records received from Mobilelink, Hayden's primary cell phone is an iPhone 11 Pro Max using phone number 972-504 5939. Based on statements of other Mobilelink employees, they believe he only has one cell phone.

CONCLUSION

31. Based on the aforementioned facts, affiant states there is probable cause to believe, and does believe, that Gregory Pierre Hayden has violated and attempted to violate, Title 18, United States Code, Sections 1028(a)(7) (fraud and related activity in connection with identification documents, authentication features, and information), 1030(a)(5)(A) (fraud and related activity in connection with computers), 371 (conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(5)(A)) and 371 (conspiracy to commit fraud and related activity in connection with computers as it relates to 18 U.S.C. § 1030(a)(4)).

DAVID KO
Special Agent FBI

Sworn and subscribed to me by phone, on this 11th day of June, 2020, and I find probable cause,

Dena Palermo

DENA HANOVICE PALERMO
UNITED STATES MAGISTRATE JUDGE